Template Version Number: 01-2021

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Impact Assessment
for the
NOAA8203
National Weather Service Performance Management System (N-PMS)

Reviewed by: Mark Graff Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

GRAFF.MARK.HYRUM.1514447892
Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2023.06.27 14:19:05 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment NOAA/ NWS/ Performance Management System (N-PMS)

Unique Project Identifier: NOAA8203 006-48-01-12-02-3118-00

Introduction: System Description

NOAA8203, referred to as "NWS Performance Management System (N-PMS)," measures the accuracy and timeliness of National Weather Service warnings and forecasts issued for the public, aviation, marine, fire weather, and emergency management communities. Additionally, N-PMS is the NWS source for all Government Performance and Results Act (GPRA) Modernization Act of 2010 metrics.

NWS employees monitor forecast and warning performance at their forecast office predominantly use the N-PMS website. A subset of these users also access the Performance Management website to conduct data entry interactions for programs such as Storm Data and the NWS Outreach and Education Event System. Access to the N-PMS data is prohibited without logging in to the Performance Management website with a valid user account. System administrators must approve each user account request before access is granted.

Occasionally external partners from other government agencies or academic institutions (i.e., non-NOAA entities) will work with the NWS on data analysis projects and require access to the Performance Management website. In these situations, the Performance Management website administrators initiate the account registration process with these partners by sending an account registration form via email. All users (internal and external) must have a valid e-mail address to proceed through the account request process. The external partners fill out the N-PMS account request form with their contact information, including a statement describing why they need access to the website, and submit the form back to the N-PMS system administrators. N-PMS system administrators review the information within the user account request and either reject or approve access to the user. Only after the user account request is approved will the external user be granted an account to log in to the N-PMS website.

To provide the users with a customized experience on the N-PMS website, and to ensure that Storm Data and the NWS Outreach and Education Event System data submissions are attributed to correct user's correct duty station, the user creates their own unique username. General information is also collected during the account registration process. The user is required to provide their first and last name, email address, duty station, and title. The user may also enter their work address and work phone, but providing this contact information is optional. When the user enters their information into the N-PMS registration page, it undergoes input validation to ensure that each data entry is accurate and to protect the system against malicious code injection or duplicate account creation. Input is validated for format, maximum/minimum length, and input type. After the information is verified, the system uses a stored procedure to validate that the user has entered a unique username and a unique noaa.gov email address. If either the username or the noaa.gov email are not unique, the system displays an invalid entry message to the user and prompts for re-entry. Once a unique username is chosen and a unique noaa.gov email is entered, the system adds the user account to the system database and the user registration is complete. Upon completion, an email alert is sent to the N-PMS system administrator and a notification email is sent to the user.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

NOAA8203 is a General Support System.

(b) System location

Silver Spring, MD

Kansas City, MO

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

Interconnects with NOAA8850 for basic network connectivity to NOAA and the internet and NOAA0100 for use of NOAA enterprise security tools.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Users access the Performance Management website to conduct data entry interactions for programs such as Storm Data and the NWS Outreach and Education Event System.

(e) How information in the system is retrieved by the user

Through the secure website using their authorized user account.

(f) How information is transmitted to and from the system

Data is submitted securely through the website and stored in an encrypted Microsoft SQL database. It is backed up onto Google Drive regularly.

(g) Any information sharing

NWS employees monitor forecast and warning performance attributed to their forecast office predominantly by using the N-PMS website. A subset of these users also access the Performance Management website to conduct some data entry interactions for programs such as Storm Data and the NWS Outreach and Education Event System. No one is allowed access to data without logging into the Performance Management website with a valid user account. System administrators must approve each user account request before access is granted. Occasionally, external partners from other government agencies or academic institutions (i.e., non-NOAA entities) will work with the NWS on data analysis projects and require access to the Performance Management website. All users must have a valid e-mail address. In these situations, the Performance Management website administrators initiate the account registration process with these partners by sending an account registration form via email. The external partners complete the account registration form with their contact information, including a statement on why they need access to the website, and submit the form back to the administrators. Only after the website administrators review the contact information and access statement and approve access will the external user be granted an account to log in.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The legal authority for civil service employment is 5 U.S.C. 301, Departmental Regulations. For the data provider information, 5 U.S.C. 301 and 15 U.S.C. 1512, Powers and duties of Department [of Commerce], are applicable.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Low

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non- Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number	x	r. Criminal Record	
e. Age		l. Email Address	x	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	

g. Citizenship		n. Religion			
u. Other general personal data (specify): Latitude and longitude location of individual					

Work-Related Data (WRD)					
a. Occupation	x	e. Work Email Address	x	i. Business Associates	
b. Job Title	x	f. Salary		j. Proprietary or Business Information	
c. Work Address	x	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	x	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	x
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
State, Local, Tribal	x	Foreign	x		
Other (specify): Military (e.g., .MIL), Foreign Educational Institutions (e.g., .EDU.AU for Australia).					

Non-government Sources					
Public Organizations		Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Some N-PMS website users, approximately 150 of the 3700 total users, voluntarily enter weather event data in the form of latitude and longitude coordinates of weather events. When the coordinate data is entered, it is accompanied by the user's first initial and last name. If users find errors in their user information or if an error occurs during data entry, it can be corrected by contacting the main system administrators.

NOAA8203 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise services for audit log management and vulnerability analysis.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
x	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			
x	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	x
For web measurement and customization technologies (single-session)	x	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

PII/BII is used for user verification and a contact list. Information is not used differently based on the type of user (i.e., government, contractor, and student).

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

One potential threat to privacy is that users could determine another user's physical location by corresponding a name or initials with a latitude/longitude location of weather events being reported. However, the large majority of N-PMS users are NOAA internal user, so this information could be obtained by publicly available information or by looking at their email contact cards.
There is also the possibility of insider threat.
Data handling and retention security controls are in place that ensure the information is handled, retained, and disposed appropriately.
There is also a Privacy Policy, which can be found on the web pages at: https://verification.nws.noaa.gov/services/public/privacypolicy.aspx and all NOAA employees, NOAA contractors, and NOAA temporary users must take the NOAA IT Security Awareness Training annually. NOAA8203 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise services for audit log management and vulnerability analysis.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
x	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

x	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA8850 and NOAA0100; access controls are in place so that only NOAA8203 personnel can access PII within the secure databases.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://verification.nws.noaa.gov/services/public/privacypolicy.aspx

.

x	Yes, notice is provided by other means.	Specify how: Notice is provided in the email sent to prospective account users by NWS.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Applying for an N-PMS account is voluntary. If a person does not want to set up an account, he/she will not provide the information requested by NWS.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Applying for an N-PMS account is voluntary. There is only one use for this PII. If a person does not want to set up an account, he/she will not provide the information requested by NWS.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users can update their profile once an account has been established by logging into the Performance Management website. The account update interface on the Performance Management website allows the user to change their name, e-mail address, phone number, job title, and office. This information is provided on the opening web page.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:**
x	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 6/27/22 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
x	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

- Physical and logical access to PII is restricted to authorized personnel only.
- NOAA8203 has no output devices (e.g., printers and audio devices). All monitors are operated under controlled space.
- NOAA8203 servers are located in keycard access controlled computer rooms.
- Remote access to NOAA8203 is only possible via secure VPN while using CAC-enabled GFE or system approved devices
- Encryption is used for PII within the database.
- Physical media is sanitized prior to disposal or reuse.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g,, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission; COMMERCE/DEPT-18, Employees Files Not Covered by Notices of Other Agencies, COMMERCE/DEPT-25, Access Control and Identity Management System. COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: 2.1 Employee Acquisition Records 2.2 Employee Management Records 2.3 Employee Relations Records 2.4 Employee Compensation & Benefits Records 2.5 Employee Separation Records 2.6 Employee Training Records 2.7 Employee Health & Safety Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal

Shredding		Overwriting	
Degaussing	x	Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

x	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

x	Identifiability	Provide explanation: Since name and phone number are publicly available, there would be low adverse effect to individuals if that information was accessed or disclosed from NOAA8203.
x	Quantity of PII	Provide explanation: Due to the nature of the PII, the impact would be low
x	Data Field Sensitivity	Provide explanation: NOAA8203 does not maintain sensitive PII information on the system
x	Context of Use	Provide explanation: Based on NOAA8203's context of use described in Section 5.1, there would be low impact if information was accessed or disclosed.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Access to PII is described above in Section 8.2. Physical and logical access restrictions are in place as prescribed in NIST 800-53. No PII is stored on mobile devices.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the

choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

One potential threat to privacy is that users could determine another user's physical field site by corresponding a name or initials with a latitude/longitude of weather data entered. However, since names, phone numbers, and corresponding field sites are publicly available, there would be low adverse effect to individuals if this identifiable information was accessed or disclosed from NOAA8203. In addition, this information could only be accessed by privileged users, not all users. Physical and logical access to PII is restricted to authorized personnel only. NOAA8203 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise services for audit log management and vulnerability analysis.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.